WORKFORCE SECURITY AWARENESS TRAINING

SERVICE DESCRIPTION

Description of Service

This document describes BlueVoyant's Workforce Security training program offered by BlueVoyant ("BV") to its customers ("Customer", "Client", or "you") pursuant to a service order explicitly authorizing the purchase and sale of the Service. For the avoidance of doubt, the terms of BlueVoyant Master Services Agreement ("MSA") available at https://www.bluevoyant.com/bvmssterms shall govern in the absence of a master services agreement signed by BlueVoyant superseding those terms.

Service Overview

The overwhelming majority of successful cyberattacks (91%) begin with the exploitation of an employee's willingness to help or their curiosity. These are both inherently positive employee attributes that can also leave your team vulnerable to nefarious schemes to coax them into taking actions that expose sensitive data.

BlueVoyant's Workforce Security Awareness Training Program is designed to illuminate how and why your team is the number one target in cyberattacks and empower them to be the very best defense against future attacks.

The BlueVoyant Workforce Security Awareness Training Program is a unique live classroom or online synchronous program that incorporates a proprietary mix of proven techniques to ensure employees are **motivated** to improve security behavior. This is a major differentiator from programs that involve delivery of facts and knowledge regarding static security scenarios. Asynchronous online training and sporadic phishing tests are designed to just deliver facts and are a great supplement to a more robust training experience, but security knowledge is only valuable when employees are cognizant of how to apply knowledge in future scenarios and most importantly, are inspired to do so.

The BlueVoyant team offers classroom and synchronous instruction that provides the following advantages over online programs:

- Participants retain more knowledge when they are in a dedicated, focused experience led by an expert instructor. Participants in online learning often multitask, stop and start training at will, and, whenever possible, skip through training.
- A keystone of our program is that we are experts in motivating employees, not just providing facts.
- A classroom environment provides an opportunity for the instructor to see how different learners engage and then adjusts delivery accordingly.
- Instructor led, plus hands-on activities, allows participants to practice new skills in a safe environment where they can ask questions and go deeper in their understanding of how to

respond to slight variations on different security scenarios. Online programs present narrow scenarios with no opportunity to explore similar but different situations.

- Group activities such as those in BlueVoyant Workforce Security Awareness training provide participants with opportunities to engage with each other, build relationships, and reinforce learning
- Studies show that companies get better results in a condensed, shorter time frame with instructor-led training.

Further, the hands-on and practice methods used during training are proven to Increased material retention. Research shows that learners retain more when taught by demonstration and hands-on training – up to 75% more than lecture or online training modules.

Everyone learns at a different pace. If a participant is struggling with a particular concept or learning objective, the instructor can provide additional assistance during breaks or after class. This is not possible with online techniques. There is no opportunity to ask questions of a subject matter expert.

Finally, our training program is designed to build a culture of security among your team along with suggestions, tools and techniques that can be used post learning to help your team continue to grow and support each other.

BlueVoyant's Workforce Security Awareness Training Methodology

BlueVoyant will work with you to develop targeted training tailored to your operating environment and the specific cybersecurity needs. We will work hand in hand with client stakeholders to ensure training that meets the standards of all parties, is delivered effectively and conveniently, and will resonate with the target audience.

Phase 1: Design

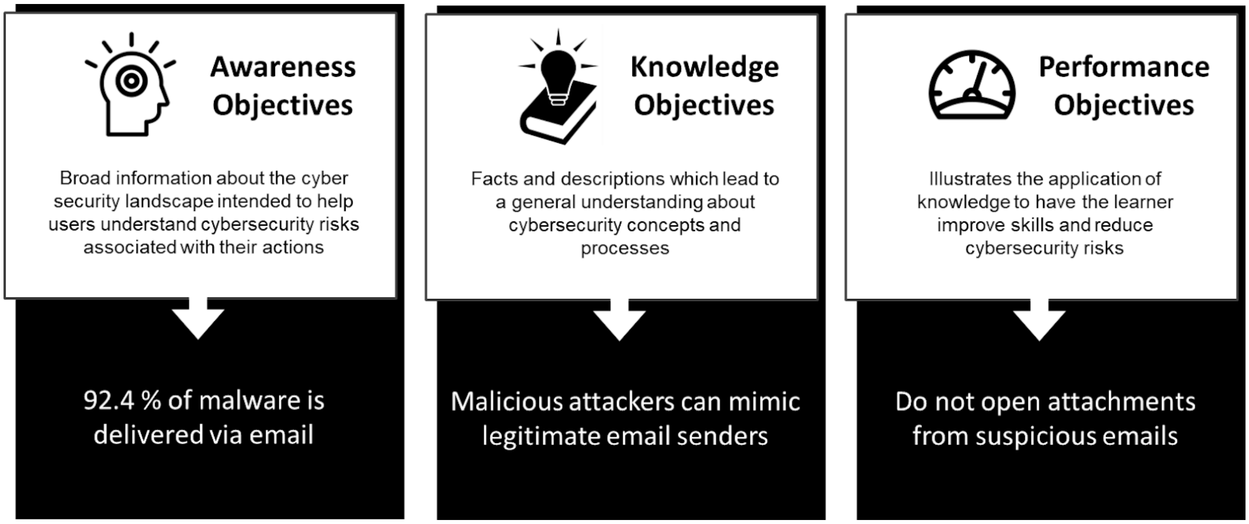
The instructional design in Phase 1 is predicated on accurate information regarding the Client's cyber security needs and target audience. BlueVoyant will collect information through discussion, interviews and observation to design training. This phase of the training process may incorporate any combination of face-to-face, virtual media, and phone conversations with selected staff. BV will use this information to customize and develop learning objectives for the training.

These objectives typically include some combination of creating awareness, imparting deeper knowledge on particularly important subjects, motivating the team to take action, and identifying performance objectives for the target audience. A unique aspect of our training is the ability to include a broader set of customization options. The following table presents representative customizations that our clients have available to them through our program.

Table of Representative Training Customizations

♦ Regulatory training (HIPAA, GDPR, CMMC)	♦ 3rd Party Organization Risks	♦ Information Security While Traveling
♦ Social Media Best Practices	♦ Spearphishing/Phishing	♦ BYOD
♦ Social Engineering	♦ Safe Internet Habits	♦ Removable Media
♦ Physical Security	♦ Deep Fakes	♦ Phone Scams
♦ Clean Desk	♦ Working from Home	♦ Password attacks/management
♦ Executives as Targets	♦ Data Privacy	♦ Dark Web Basics
♦ Security Roadmap & Business Risk	♦ Cyber Insurance Selection	♦ SMS and Texting Security

Once objectives are identified, a customized, unique training program is then developed for the specific target participants.



Awareness Objectives

Broad information about the cyber security landscape intended to help users understand cybersecurity risks associated with their actions

92.4 % of malware is delivered via email

Knowledge Objectives

Facts and descriptions which lead to a general understanding about cybersecurity concepts and processes

Malicious attackers can mimic legitimate email senders

Performance Objectives

Illustrates the application of knowledge to have the learner improve skills and reduce cybersecurity risks

Do not open attachments from suspicious emails

Example of Learning Objectives and Application

Phase 2: Delivery

Phase 2 involves delivery of the training to the intended audience. Notwithstanding the tailoring that will occur during Phase 1, the training will focus on a high-level view of the cyber threat landscape and how the staff operates within that environment followed by specific threat actor behavior relevant to the Client. The session will then be capped by preventative and mitigating actions users can perform to secure themselves and the organization. Training is delivered via classroom techniques, including but not limited to quizzes, group work, hands-on experiences, lecture, case studies and demonstrations. The balance of activities will depend on the objectives defined in Phase 1, but all training is designed to be engaging, interactive, motivating and memorable.

Phase 3: Review

A pretest to measure baseline skills is administered at the beginning of training. In the final phase of training we measure both knowledge and motivation to improve habits to determine training retention. The final review will be based on the objectives defined in Phase 1 and thus the training delivered in Phase 2. We will also develop recommendations for further training activities to include retraining, additional training topics, and future areas of focus. *Note: Final testing is done immediately following training unless otherwise specified by the client.*

BlueVoyant Workforce Security Awareness Training Service Tiers

Classroom training for employees – This is the most effective method of delivery as it allows the instructor to gauge the level of resonation with the greatest accuracy. It also offers the most robust set of learning experiences for the participants. With this method, a member of our team will come to your company to deliver training face-to-face. Quizzes are used before training for baseline measurement and afterwards to measure change in participant understanding.

Online synchronous training for employees – This is very similar to the classroom training experience with a member of our team delivering training via an online synchronous platform instead of face to face, with some limitations on the level of interactive methods that can be employed. There are, however, no limits on the scope of content that can be delivered with this approach to learning.

In addition to synchronous instruction, BlueVoyant can provide visual aids including posters for various locations throughout the office, documentation of lessons learned and related organizational policies as supplements to the training.

Training services can be provided for various levels of participants. Training can be provided for the entire organization or for a specific set of target participants such as executives or employees who handle a particular type of sensitive information.

Client Responsibilities

A member of our team will work with one or more client stakeholders or subject matter experts to understand the specific target security behaviors that should be addressed in the training program. We will prepare a recommendation for length and scope of security training. If the security awareness training is to be completed onsite, the client is responsible for identifying an appropriate venue and ensuring the safety and comfort of participants. The Client is also responsible for ensuring participation of the target team members and ensuring that team members are adequately prepared with the devices and materials needed to complete the program.

The Client is responsible for designing and enforcing the company policies that define expected team member participation in the program.

Specific metrics and implementation methods for objectives are the responsibility of the BlueVoyant team but the Client is responsible for final sign off on the adequacy of the objectives and metrics prior to delivery of training.